УДК 378.6:519.83

Студ. Н.Ю. Савось
Науч. рук. доц. И. К. Асмыкович
(кафедра высшей математики, БГТУ)

ПРОБЛЕМА КЛАССОВ P И NP

Вопрос о равенстве классов сложности P и NP (в русских источниках также известный как проблема перебора) — это одна из центральных открытых проблем теории алгоритмов уже более трёх десятилетий (проблема института Клея, за решение которой дают вознаграждение). Если на него будет дан утвердительный ответ, это будет означать, что теоретически возможно решать многие сложные задачи существенно быстрее, чем сейчас.

P класс

В теории алгоритмов классом P (от англ. polynomial) называют множество задач, для которых существуют «быстрые» алгоритмы решения (время работы которых полиномиально зависит от размера входных данных).

Формальное определение

Алгоритм отождествляется с детерминированной машиной Тьюринга, которая вычисляет ответ по данному на входную ленту слову из входного алфавита ∑. Временем работы алгоритма $T_m(x)$ при фиксированном входном слове x называется количество рабочих тактов машины Тьюринга от начала до остановки машины. Сложностью функции f: ∑∗ → ∑∗, вычисляемой некоторой машиной Тьюринга, называется функция $C: N \to N$, зависящая от длины входного слова и равная максимуму времени работы машины по всем входным словам фиксированной длины

$$C_M(n) = \max_{x:|x|=n} T_M(x).$$

Если для функции f существует машина Тьюринга M такая, что $C_M(n) < n^c$ для некоторого числа c и достаточно больших n, то говорят, что она принадлежит классу P, или полиномиальна по времени.

Задачи, принадлежащие классу P

Примерами задач из класса P являются целочисленное сложение, умножение, деление, взятие остатка от деления, умножения матриц, выяснение связности графов, сортировка множества из n чисел, нахождение эйлерова цикла на графе из m рёбер, обнаружение в тексте длиной n некоторого слова, построение покрывающего дерева

минимальной стоимости, линейное программирование и некоторые другие.

NP класс

В теории алгоритмов классом NP (от англ. non-deterministic polynomial) называют множество проблем разрешимости, решение которых возможно проверить на машине Тьюринга за время, не превосходящее полинома от размера входных данных, при наличии некоторых дополнительных сведений (так называемого сертификата решения).

Эквивалентно класс NP можно определить как содержащий задачи, которые можно за полиномиальное время решить на недетерминированной машине Тьюринга.

Задачи, имеющие полиномиальные по времени алгоритмы решения, можно решать с помощью компьютера значительно быстрее, чем путём прямого перебора, время которого экспоненциально. Это обуславливает практическое значение проблемы о равенстве классов P и NP.

Определения

Класс сложности NP определяется для множества языков, то есть множеств слов над конечным алфавитом. Язык L называется принадлежащим классу NP, если существуют двуместный предикат R(x,y) из класса P (то есть вычислимый за полиномиальное время) и константа c>0 такие, что для всякого слова x условие «x принадлежит L» равносильно условию «найдётся y длины меньше |x|^{c} такой, что верно R(x,y)» (где |x| — длина слова x). Слово y называется сертификатом принадлежности x языку L. Таким образом, если у нас есть слово, принадлежащее языку, и ещё одно слово-свидетель ограниченной длины (которое бывает трудно найти), то мы быстро сможем удостовериться в том, что x действительно принадлежит L.

Эквивалентное определение можно получить, используя понятие недетерминированной машины Тьюринга (то есть такой машины Тьюринга, у программы которой могут существовать разные строки с одинаковой левой частью). Если машина встретила «развилку», то есть неоднозначность в программе, то дальше возможны разные варианты вычисления. Предикат R(x), который представляет данная недетерминированная машина Тьюринга, считается равным единице, если существует хоть один вариант вычисления, возвращающий 1, и нулю, если все варианты возвращают 0. Если длина вычисления, дающего 1, не превосходит некоторого многочлена от длины x, то предикат называется принадлежащим классу NP. Если у языка существует распознающий его предикат из

класса NP, то язык называется принадлежащим классу NP. Это определение эквивалентно приведённому выше: в качестве свидетеля можно взять номера нужных веток при развилках в вычислении. Так как для x принадлежащему языку длина всего пути вычисления не превосходит многочлена от длины x, то и длина свидетеля также будет ограничена многочленом от длины x.

Примеры задач принадлежащих NP классу

Можно привести много задач, про которые на сегодняшний день неизвестно, принадлежат ли они P, но известно, что они принадлежат NP. Среди них:

- Определение наличия в графе гамильтонова цикла. Сертификат — последовательность вершин, образующих гамильтонов цикл.
- Неоптимизационный вариант задачи о коммивояжёре (существует ли маршрут не длиннее, чем заданное значение k) — расширенный и более приближенный к реальности вариант предыдущей задачи. Сертификат - такой маршрут.
- Существование целочисленного решения у заданной системы линейных неравенств. Сертификат — решение.
- Кратчайшее решение «пятнашек» размера $n \times n$

Среди всех задач класса NP можно выделить «самые сложные» — NP-полные задачи. Если удастся решить любую из них за полиномиальное время, то все задачи класса NP также можно будет решить за полиномиальное время.

NP-полная задача — в теории алгоритмов задача с ответом «да» или «нет» из класса NP, к которой можно свести любую другую задачу из этого класса за полиномиальное время (то есть при помощи операций, число которых не превышает некоторого полинома в зависимости от размера исходных данных). Таким образом, NP-полные задачи образуют в некотором смысле подмножество «типовых» задач в классе NP: если для какой-то из них найден «полиномиально быстрый» алгоритм решения, то и любая другая задача из класса NP может быть решена так же «быстро».

Равенство P=NP может означать, что задачи, решение которых раньше считалось очень сложным, теперь решаются за полиномиальное время.

Любая криптосистема с открытым ключом базируется на предположении существования односторонних функций и/или крайней затратности решения некоторой задачи (например, для алгоритма RSA это разложение на множители очень больших чисел). В зависимости от того будет ли доказана принадлежность задач NP класса к P классу будет зависеть безопасность всех систем базирующихся на криптосистемах и задачах которые принадлежат к NP классу. То есть текущие системы безопастности базирующиеся на NP задачах построены на вере в неупрощаемость этих задач. Но это является лишь неполным условием. Иными словами, в NP-задачи заложена мера сложности «в худшем случае», но для стойкости криптографической системы необходимо, что бы задача была сложной «почти всюду». Таким образом, нам видно что для криптографической стойкости необходимо существенно более сильное предположение, чем $P \neq NP$(хоть и в большинстве случаев оно является достаточным, кроме случаев с криптосистемами с открытым ключом). А именно, предположение о существовании односторонних функций.

ЛИТЕРАТУРА

1. Введение в криптографию, В.В. Ященко 2012.- С. 348.
2. Википедия, свободная энциклопедия(https://www.wikipedia.org)
3. Д. Хопкрофт, Р. Мотвани, Д. Ульман., Введение в теорию машин Тьюринга // Введение в теорию автоматов, языков и вычислений 2002. – С. 528.

УДК 519.83

Студ. П.С. Шенец
Науч. рук. асс. Т.Г. Шагова
(кафедра высшей математики, БГТУ)

ИГРА «НИМ»

Ним – это конечная игра с полной информацией, которая является фундаментом математической теории комбинаторных игр. Эта древняя китайская игра пришла в Европу только в 16 веке, а известное нам название, одновременно с доказательством того, что у неё есть выигрышная стратегия, получила только в 20 веке. И то, и другое сделал математик Чарльз Бутон.

В 30-х годах XX в. независимо друг от друга два математика — Р. Шпраг и П.М. Гранди — разработали теорию, описывающую равноправные игры. И Ним имеет фундаментальное значение для этой теории, так как в ней утверждается, что любая равноправная игра двух игроков эквивалентна обычному Ниму.